An Energy- Efficient Optimal multi-dimensional location, Key and Trust Management Based Secure Routing Protocol for Wireless Sensor Network

S.Sudha Mercy[1*], J.M.Mathana[2], and J.S.Leena Jasmine[3]
[1] Department of Computer Science Engineering, Jeppiaar Institute of Technology, Chennai - 631 604, India.
[E-mail: sudhamercy.phd@gmail.com]
[2] Department of Electronics and Communications Engineering, St Peter's Institute of Higher Education and Research, Chennai- 600 054,India,
[E-mail: jm.mathana@gmail.com]
[3] Department of Computer Science Engineering, Velammal Engineering College, Chennai- 600066, India,
[E-mail: leenavictorece@gmail.com]
[*]Corresponding author: S.Sudha Mercy

Received November 30, 2020; revised May 29, 2021; revised July 21, 2021; accepted August 10, 2021; published October 31, 2021

Abstract

The design of cluster-based routing protocols is necessary for Wireless Sensor Networks (WSN). But, due to the lack of features, the traditional methods face issues, especially on unbalanced energy consumption of routing protocol. This work focuses on enhancing the security and energy efficiency of the system by proposing Energy Efficient Based Secure Routing Protocol (EESRP) which integrates trust management, optimization algorithm and key management. Initially, the locations of the deployed nodes are calculated along with their trust values. Here, packet transfer is maintained securely by compiling a Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC) approach. Finally, trust, key, location and energy parameters are incorporated in Particle Swarm Optimization (PSO) and meta-heuristic based Harmony Search (HS) method to find the secure shortest path. Our results show that the energy consumption of the proposed approach is 1.06mJ during the transmission mode, and 8.69 mJ during the receive mode which is lower than the existing approaches. The average throughput and the average PDR for the attacks are also high with 72 and 62.5 respectively. The significance of the research is its ability to improve the performance metrics of existing work by combining the advantages of different approaches. After simulating the model, the results have been validated with conventional methods with respect to the number of live nodes, energy efficiency, network lifetime, packet loss rate, scalability, and energy consumption of routing protocol.

Keywords: WSN, Optimization, Energy Consumption, Network Routing Protocol, Clustering

1. Introduction

Wireless Sensor Network (WSNs) plays a significant role in various applications like agriculture, healthcare, military operations and target tracking approach [1], [2]. Generally, WSNs comprises one or more sink node, low-cost and small size of sensor nodes. For instance, in the batteries system, the sensor nodes have inadequate energy sources. Due to the unattended and complexity of deployments of sensor nodes, recharging the energy source of the sensor node manually is challenging [3], [4]. Owing to these causes, the design of WSNs protocol along with reduced energy utilization of sensor node has become a complex issue [3]. Also, there is an absence of security approaches whereas transmitting the data outside the network or storing the data inside the system might be causing the loss of data integrity and privacy [5]. Such a domain raises security genuinely relating to the protection of basic information combined with the asset restrictions of the individual sensor hubs [6], [7]. But, WSNs have a few sets of constrained hubs that make secure protocols than traditional networks with respect to CPU usage, memory and energy consumption [8]–[10]. To relieve the security issues of this standard then fulfil the information secrecy and trustworthiness prerequisites of the WSNs [11], the various cryptographic technique has been suggested in the available literature studies. The viability of cryptographic security is used to attain a great extent which relies on the basic key management (KM) technique [12], [13]. For instance, there are different key management schemes proposed that applies channel, key distribution, key generation based on biometric or clock-based approach, KM and key refreshing operations, cryptographic, and key agreement approach. However, the majority of those methods depends on the key management approach [14]. However, none of the researchers have considered the combination of trust management, security issues and KM in the WSNs and this study is a first of its kind which investigates all of these combinations in the WSNs to mitigate the above challenges. This study has been structured as follows. This section has given a brief introduction to the research, followed by the background of the concepts which is given in Section 2. The review of literature is presented in Section 3 where the previous studies have been studied and the research gap is identified. The proposed EESRP model, system architecture, trust and key management working principles are discussed in section 4. The simulation results, evaluation metric, comparison of studies, along with a summary of obtained simulated outcomes, are discussed in section 5. The results are then discussed and inferred in section 6. At last, the findings and conclusion of the proposed EESRP approach are presented along with the recommendations in section 7.

2. Background

The Harmony Search (HS) approach is an evolving metaheuristic algorithm of optimization, used throughout the previous decade to deal with many difficult situations. In the last decade, several updated HS algorithms were explored to improve the original version's performance. The stochastic derivatives allow the possibility of selecting particular discrete variables throughout the HS process of development. It is effective in handling discrete optimization issues and has been used to design fluid transport networks optimally. The population-based stochastic technique to tackling constant and discrete issues in optimising particles is PSO. Simple software agents, termed particles, travel into the search space of an optimization problem during particle swarm optimization. A particle's location is a candidate's answer to the issue of optimization. Each particle seeks a better search space location by adjusting its speed according to principles originating from behavioural bird-flocking models. Optimizing

particle swarms is a type of swarm intelligence method used to tackle issues using optimization.

3. Related Work

Generally, most of the routing protocols' primary focus is to attain power conservation in WSNs [15]–[18]. With regards, some of them focused on the energy-efficient routing protocol [19]–[21], energy-efficient cluster-based routing protocol [22]–[25], trust with key management based routing system for achieving high security [26], [27], and optimization based routing technique with security [28]–[31]. The summary of these methods is discussed as follows.

Similarly, research by Sharma et al. [32] evolved a clustering routing protocol for WSNs. Furthermore, they have combined different sensor nodes, and then the resulted clusters are translated into hierarchical management systems that are having various cluster heads and base stations. The simulated results show that they attained better results in terms of end-to-end delay and energy consumption. At the end of the research, they recommended that will enhance the performance by adopting network security and privacy concern with varying environmental conditions.

A work by Mehta and Saxena [33] presented a Multi-Objective Based Clustering, and Sailfish Optimizer (SFO) guided routing approach toward sustain energy efficiency in WSNs. Based on the evaluation of fitness function, they have selected the cluster head. With regards, they have minimized the number of dead sensor nodes and minimized the energy consumption of the routing protocol. For transmission of data, the suggested model selected an optimal path while after the selection of cluster head. The suggested model performance was compared with four traditional methods namely, genetic algorithm, grey wolf optimization, particle swarm optimization method and ant lion technique with specific to packet delivery ratio, energy consumption, network lifetime, network throughput ratio. The demonstrated results show that the suggested model gives better performance while the average measure of the number of alive sensor nodes (24.4%) and energy consumption (21.9%).

A work by Sun et al. [34] presented a secure routing protocol on the basis of Multi-objective Ant-colony-optimization for WSN. By adopting the trust value of route path and residual energy, the ant colony optimization method has been enhanced. The performance of the suggested model tested using network simulator version 2 that the resulted outcome shows attain better performances in terms of average energy consumption, routing load and data packet loss ratio. But the limitation of this study as only considered the four constraints and two objective functions. So, further needs to enhance the system performance by assuming more constraints and objective function which should minimize the network failure probability, maximize the network reliability, and maximize the network lifetime

Rao et al. [35] presented a cluster-head selection protocol based on the PSO method. However, the simulated results have shown that the distance between the sink and a selected channel does not cover the uniformity of the entire region, which causes unstable energy intake in the network layer. Similarly, a study by Adnan et al. [36] presented a cuckoo search clustering method, whereas they incorporated two sensor nodes of different sorts. The simulated result shows that the suggested protocol consumes higher energy for 20% nodes than the left behind 80% nodes. However, it is suffered as unbalanced energy consumption from non-uniform Channel distribution problems in the network. A study by Elhabyan and Yagoub [37] presented a two-tier PSO based routing and clustering protocol. But these approaches also suffered from unbalanced energy consumption issues and have not considered balanced energy consumption.

In some cases, most of the researchers have assumed both routing and clustering protocol in the isolated entity module. Subsequently, in very few cases, the network channels are directly communicated with a sink node. But, in large-scale WSNs, the network channels are required to communicate with a sink node via multi-hop communication [38]. Hence, they have integrated the optimization issues with routing and clustering protocol via an efficient meta-heuristic approach. A work by Ahmadi et al. [39] developed the QoS (Quality of Service) routing technique for handling the energy and delayed constraints in the MANET by utilizing CA (Cellular automata) and the Genetic algorithm (GA). The proposed algorithm has enhanced network lifespan and end-to-end delay than the conventional QoS technique. Moreover, they suggested the future work might be focused on improving the packet delivery and the implementation of another QoS constraint such as the bandwidth for validating the proposed algorithm. A work by Sheng et al.
Sheng et al. [40] Presented an energy efficiency based Dynamic Source Routing protocol (DSRP) for MANETs. The experimental results demonstrated that can extends the network lifetime without incorporation of network burden. But this approach does not expose the overhead which is generated from the network. A study by Sugandh and Panday [41] has been extended the lifetime of the network path and nodes via energy-efficient LEACH protocol. Moreover, it has a low packet loss rate and high energy efficiency through the selection of cluster head. The drawback of the suggested method has more communication overhead.

From the above review, it has been observed that most of the routing protocols have failed to categorise the various factors like QoS aware, cluster-based routing protocol, postured based routing protocols, and thermal-aware, security-aware and cross-layered based routing protocol. So the study needs to focus on solving the various routing problem by considering appropriate factors like path loss, energy efficiency, latency and network node stability ratio [42]. In addition, for addressing the issues of energy consumption, a few of the researchers suggested computing-based approaches [38], cuckoo search [36], PSO [35], [37] techniques. However, these algorithms face the issues of unbalanced and balanced energy consumption problems. Also, none of them has focused all these routing protocols on a single network. So, the present study planned to propose an efficient routing protocol which is a combination of trust, key and optimization methods toward solving the various routing issues by considering the related factors namely path loss, energy efficiency, latency and network stability.

4. Proposed EESRP security approach

This research presented an improved model where we considered both security and efficiency of the system via proposing a routing protocol that integrates key management, trust management and optimization approaches. Initially, the network nodes are being deployed, and the location/position of each node is calculated. Then, the entire node trust score is intended on the basis of its location, updated trust score, node honesty ratio, frequently visited nodes and energy of nodes. Furthermore, the fuzzy rules are created, and the cluster-head is formed based on the selected cluster in the network node that has a higher trust score. To enhance the security level of the packet transfer, ECC and DSA scheme is used. Finally, trust, key, location, and energy parameters are incorporated in the PSO (particle swarm optimization) and Harmony Search based meta-heuristics techniques to find the secure shortest path. Finally, the results have been validated with conventional methods with respect to measuring of various factors such as network lifetime, number of alive nodes, total energy consumption, packet loss rate, energy efficiency, and scalability. The proposed system architecture is illustrated in **Fig 1**. The list of notations used in this section is given in **Table 1**.

Table 1. List of Notations

$D(i,j)$	Distance	RR	Route Request
L	Length of the monitoring area	RRE	RRE- Route Reply
$t(i,j)$	trust value	SF	Successful transaction,
l	The sequence evaluation records	FR	Failure transaction
d_t	Direct node	i	it denotes the particle index,
d_t (i,j)	Node trust score of node j for i	v_i	It denotes a velocity of i^{th} particle,
N	No.of the neighbour node.	Φ	It denotes inertia function
α and β -	weighed factors related to security policies.	$\alpha_{1,2}$	It represents an acceleration constant and
$dt_{P(j)}(i,j)^{l-1}$	Direct node trust score based on past behaviour of network node	P_i	It denotes the best position, which is found via i^{th} particle,
$dt_{N(j)}(i,j)^{l-1}$	Direct node trust score w.r.to past malicious node.	$\gamma_{1,2}$	It denotes the generation of random numbers to i^{th} particle.
$\gamma 1$ and $\gamma 2$	A positive and negative assessment based on the exponential decay time factor	G	It represents the best position which is obtained via swarm (global best),
it (k,j)	It represents the indirect trust score of the node (node k and j).	x_i	It denotes the i^{th} position of particles,
dt(i,k)	It denotes the direct node trust score of I (node i and k).	dt(k,j)	It denotes the direct node trust score (j and k)

4.1 System Architecture

In a wireless sensor network, the suitable route has been predicted based on the selection of neighbour nodes which is responsible for data transfer between the source to the endpoint. Furthermore, the neighbour node is selected based on attained trust value and node distance.

4.2 Trust Management

Initially, the nodes are deployed, and the location/position of each node is calculated. Then, the entire node trust score is measured based on its location, updated trust value, node honesty, frequently visited nodes and node energy. Whereas the trust value is used finding a stable route amongst source and destination node. Subsequently, the clusters and fuzzy rules have been created by selecting the cluster head with respect to the network node that was having a high trust value. The performance of the trust management is measured by packet drop rate, packet transmitted rate and receiver rate. On the other hand, describe whether it's a successful transmission or a failure.

In our study, the distance amongst the node has been measured by,

$$D(i,j) = \sqrt{[(x_1 - x_2)^2 + (y_1 - y_2)^2]} \quad (1)$$

Here the term distance D is measured based on the source and destination node whereas j coordinate with y_2 and x_2, and i coordinate with y_1 and x_1.

Threshold area for neighbour nodes = L/2.

Where, L- length of the monitoring area

The overall trust score of two nodes, i.e. destination node and source node has been measured by interactions amongst neighbouring and source node of the entire network system. With the help of neighbour node, the overall trust score is measured which is mathematically written as,

$$t(i,j)^l = \alpha dt(i,j)^l + \beta \frac{\sum_{(k \in Cj, k \neq i)}^{n} it(k,j)^l}{n-1} \quad (2)$$

Here t (i,j) denotes the trust value of two nodes, i.e. j node for i.
it (k,j) denotes the k- node that has its place to Nbr_N j

l - The sequence evaluation records.

d_t – Direct node which is measured by past and present Nbr_N direction
d_t (i,j) – Node trust score of node j for i
n – No.of the neighbour node.
α and β - weighed factors related to security policies.
It is to be noted, dt of a node is frequently updated in a database once done with every failure or success communication, and the obtained results are measured as:

$$dt(i,j)^l = \gamma_1 dt_{P(j)}(i,j)^{l-1} + \gamma_2 dt_{N(j)}(i,j)^{l-1} + ids(i,j)^l \quad (3)$$

Whereas,

$dt_{P(j)}(i,j)^{l-1}$ - Direct node trust score based on past behaviour of network node
$dt_{N(j)}(i,j)^{l-1}$ - Direct node trust score w.r.to past malicious node.
$\gamma 1$ and $\gamma 2$ - A positive and negative assessment based on the exponential decay time factor

The device current measurement behaviour is defined as,

$$ids(i,j) = \begin{cases} P(j), 0 < P(j) < 1 \\ 0, uncertain \\ N(j), -1 < N(j) < 0. \end{cases} \quad (4)$$

Whereas, the term N (j) and p (j) denotes the evaluation of j device (Positive and negative manner). The indirect trust score is measured by without straight interactions of network nodes and obtained trust score amongst distributed nodes. The indirect trust score of a sensor network is defined by,

$$\sum_{(k \in Cj, k \neq i)} it(k,j)^l \equiv \sum_{(k \in Cj, k \neq i)} \left(dt(i,k)^l dt(k,j)^l \right). \quad (5)$$

Here

it (k,j) – represents the indirect trust score of the node (node k and j).
dt(i,k) – denotes the direct node trust score of I (node i and k).
dt(k,j) – denotes the direct node trust score (j and k)

From the above steps, the trust score of the neighbour node can be computed by measuring the trust metric values. Subsequently, the next node will be chosen based on the sensor node and trust score. In this regard, the routing path is discovered. To calculate the reply, transmission, and request rate of the node by intermediate values such as RQ_i, RP_i and DT_i. It's mathematically written as given below [43],

$$RQ_i = \sum_i^n \frac{S_1 - F_1}{S_1 + F_1}; \quad (6)$$

$$RP_i = \sum_i^n \frac{S_2 - F_2}{S_2 + F_2};$$

$$DT_i = \sum_i^n \frac{S_3 - F_3}{S_3 + F_3}$$

The sensor node Trust Level Value is defined as,

$$TV = T(RR) * RQ + T(RRE) * RP + T(DATA) * DT$$

$$T_i^{trust} = T_{i^l}^{SR} t * T_{i^l}^{FR} \tag{7}$$

Where, T - time factorial of RR, RRE, DATA sent respectively.

RR-route request; RRE- route reply

$$p_i^{location} = l_t$$

Where, l denotes a specific area of network

The Trust-Threshold of sensor node is measured by,

$$TTV = \sum_i^n \frac{TV}{n} \tag{8}$$

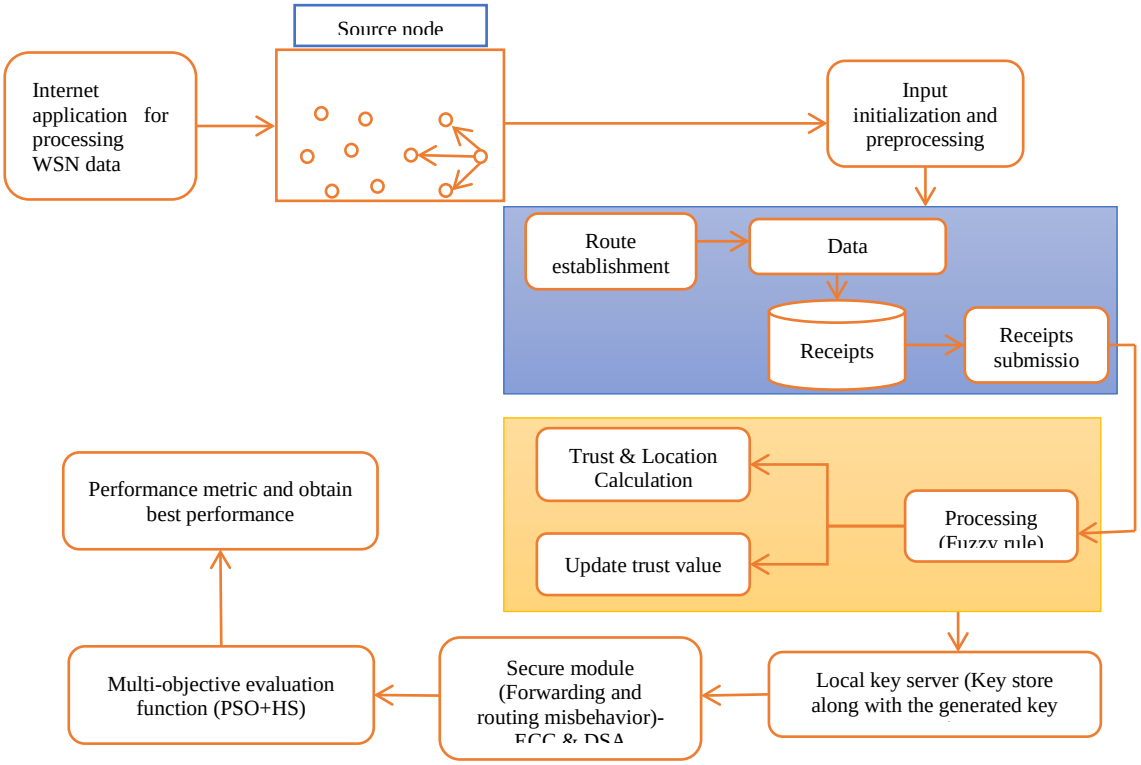

Fig. 1. Overview of proposed EESRP method

Fig. 1 shows the overview of the proposed EESRP method. The wireless sensor nodes are given as input to the source nodes. The data is then initialized and pre-processed. Fuzzy logic is used for processing the data, and then the trust value and location value is updated based on the fuzzy value. The key and value pairs are then updated for securely encrypting the data using Elliptic-Curve Cryptography (ECC) and Digital Signal Algorithm (DSA). Then the nodes are optimized using a combination of multi objectives functions which are PSO and HS. The normalized intermediate values are varied between -1 to 1. Here the high values denote the failure rate, which might be not possible to the routing. The trust threshold value (TTV) is measured by the average ratio of trust node value which is the part routing wherein trust value (TV) is measured by the entire node for the duration of routing, and it's validated as in contradiction of TTV. During the analysis, the lower threshold value denotes the probability of drop packets for the present network packet transmission and is not appropriate for the routing so needs to choose the alternate path. The significance of the proposed EESRP approach is that there it combines fuzzy processing with various algorithms like routing based modules and multi-objective functions.

4.3 Key Management

In this study, a hybrid key management technique has been utilised, which is a combination of ECC and DSA. During the file encryption process, the key pair (private and public) has generated on the basis of a random positive integer then the resulted as ciphertext format. To, decrypt the cypher-text the pair of first points is multiplied via private key, and the result has been subtracted from the second point. Here, both encryption and decryption have been adopted key size as 163 bits where encryption is done by a public key and decryption by a private key. The performance of key management technique has been validated with respect to the measure of Packet delivery ratio (PDR), Key Size Generation, Encryption and Decryption throughput, and time is taken for key Generation.

Calculate Inertia Function $\Phi(X)= (a-1)(b-1)$ and $X=a.b$

Select encryption key ‘f’ like $1<f< \Phi(X)$ and $Xm(f, \Phi(X)) =1$

To find decryption key ‘D_k’,

$f.D_k = 1 \bmod \Phi(X)$ where $o \leq D_k < X$

Hash memory is calculated based on the,

$M = \text{Hash}(a) \bmod n$

A public encryption key is measured by PEK={f,X}

Private decryption key is obtained by PDK= {D_k, a,b}

The signature has been computed by,

S= PEK (X, I); where I-integer

The presented cryptography comprises high speed, is strong in security level and generated key size is smaller.

4.4 Optimization Technique

To find the secure shortest path, PSO has been combined with HS based meta-heuristics techniques. Here, velocity moved in the search space, and entire particles are allocated with the random position. To attain the global best resolution, the particle positions and velocity have been updated with respect to the global and best value of the sensor node. Thus, the hybrid approach might manage the load stability ratio of consumed power amongst sensor nodes and wireless network path selection. Hence, the lifetime of a network node is increased as well as able toward keeping the least energy level amongst sensor nodes. In addition, paths

are continuously monitored with respect to distance, time and cost as well as update the information at continuous time events through the fitness function of each node. Additionally, the fitness position of each particle has been calculated, which helps in obtaining the efficient path via pre-defined fitness functions.

Furthermore, the performance of energy consumption has been optimised, and the intra-cluster distance of the node has been reduced by applying HS. Generally, the PSO comprises the parameters tuning performance where the HS algorithm randomly discovers search space wisely and efficiently in the network. So, the particle swarm and randomization has been combined, which increases the search space and minimizes the distance. Specifically, using a harmonic vector, the path has been created based on priority value, which corresponds to the variable nodes via optimal solution as well as enhances the performance of harmony algorithm. Then the shortest route is obtained via iterative update of harmony memory banks. Moreover, the energy efficiency of the optimization approach is restrained by various factors namely residual energy of sensor node (SN), bandwidth, intra-cluster distance, harmony memory size, energy consumption, harmony memory considering rate and path length.

In a multi-dimensional hunt space, the swarm particles are moved and have their own network node position vector and velocity, which are defined as follows Sheikhan and Hemmati [44]:

$$v_i(k+1) = v_i(k) + \gamma_{1i}(P_i - x_i(k)) \tag{9}$$

$$x_i(k+1) = x_i(k) + v_i(k+1) \tag{10}$$

Here, k represents a discrete-time index,

x_i denotes the i^{th} position of particles,

G represents the best position which is obtained via swarm (global best),

i denotes the particle index,

v_i denotes a velocity of i^{th} particle,

P_i denotes the best position, which is found via i^{th} particle,

$\gamma_{1,2}$ denotes the generation of random numbers between the interval of [0,1] functional to i^{th} particle.

The velocity is measured based on the below equation, which is from Shi and Eberhart [45], Sheikhan and Hemmati [44]:

$$v_i(k+1) = \phi(k)v_i(k) + \alpha_1\left[\gamma_{1i}\left(P_i - x_i(k)\right)\right] + \alpha_2\left[\gamma_{2i}\left(G - x_i(k)\right)\right] \tag{11}$$

Here

$\alpha_{1,2}$ represents an acceleration constant and

Φ denotes inertia function.

For searching global optima, swarm intelligence is used where all the particles have a node velocity and fitness value. Among the particles, the g-best denotes global best position and p-best called the local best position. to modernize the node position and particle velocity of the sensor node[46], which is defined as

$$v_i(t) = v_i(t-1) + c_1 r_1 + \left(localbest(t) - x_i(t-1)\right) + c_2 r_2\left(globalbest(t) - x_i(t-1)\right) \tag{12}$$

Where,

r_1, r_2 represents a random vector and

c_1, c_2 denoted as acceleration coefficient.

$$x_i(t+1) = x_i(t) + v_i(t+1) \tag{13}$$

Where,

t represents a discrete-time step,

X_i represents a particle position of i^{th} search space at time step t;

By adding the velocity v_i (t) which denotes the present location, whereas the position of each particle is varied. Once the data initialization procedure is completed, the harmony memory initial size is generated. Harmony Memory HM is measured using the equation below [19],

$$H_M = \begin{bmatrix} x_1 \ldots . x_n & f(X) \\ x_1^{H_M} \ldots . x_n^{H_M} & f(X^{H_M}) \end{bmatrix} \tag{14}$$

Furthermore, trust optimization has been measured by,

$$T_{OPT}(t+1) = t(i,j) + v_i(t) + x_i(t+1) + T^{trust}{}_i * H_M * M \tag{15}$$

Here, the trust optimization is measured by trust score, harmony memory and hash function of each sensor node (N). Regarding this, the optimization performance of the entire sensor network has been enhanced. The optimized node value is obtained by the measure of trust node and hash functionality where the trust depends on the successful interaction amongst nodes. This will enhance the node reliability of a network. Here the trust score of individual nodes is,

$$T(i,j) = SF(i,j)/(SF(i,j)+FR(i,j)) \tag{16}$$

This trust score depends on the communication behaviour and data consistency of the sensor node.

SF- successful transaction,

FR- Failure transaction

In addition, the New Harmony vector is generated as,

$$Y' = (x_1', x_2', x_3') \tag{17}$$

If the ratio of new vector fitness is optimal than the existing node, there is a need for replacing the worst harmony, which is HM with x. The stopping criteria are applied when we obtain the maximum iteration with optimal results. The proposed EESRP mathematically is written as,

$$EESRP = p_i^{location} + T_i^{trust} + CH + D + T_{OPT}.v_i + x_i + H_M \tag{18}$$

Proposed algorithm

Begin

N_t =Nodes in the network

i=ID of a SN in the present protocol

N [i].stat=start_state

for N [i]

receiver or destination node R_r from Nbr_N N_r

N[i].Info_table updates

% Parameter initialization: Trust& location calculation and key pair generation

for N i< I Di do

nonceij =random();
Select arbitrary group X_i;
C=EKv(nonceij ||X_i)
n_i→P Req, I D_j:C

$$T_i^{trust} = T_{i^l}^{directhonesty} t * T_{i^l}^{directcooperation}$$

$$p_i^{location} = l_t p_i^{location} = l_t p_i^{location} = l_t$$

Whereas, l denotes a specific area of network
% Analysis through fuzzy rule (FI)
probability (P)=FR(node[i].ND
Send Head_compete to all Nbr_N(neighbour node)
Nbr_N[j]=list of Head _compete from Nbr_N

% compare the outcome of fuzzy rule with Nbr_N.

```
If (N[i].P> Nbr_N[j].P)
        N[i].statement=CH
        advertise CH_Message
 else
        received CH_Message and choose
appropriate CH

        send N_JOIN to the nearest CH
  end
```

% ECC and DSA
Generate two primary no. and Calculate X=a.b and Φ (X)= (a-1)(b-1)
Public encr and private decryp.
% Optimization (PSO and HS)
While (Population Size)
{
Probability=FR (node[i].ND
Neighbor_Node[j]
To attain fitness value (FV)
Pbest is attained once FV is better from optimal results
Revise pbest with New_pbest
Particle selected from gbest
Initialize number of particles and harmony-memory (HM)
Create New_Harmony
Revise HM
Public encryption
Private decryption
While maximum iterations are not attained
{
For each particle in the network measure particle velocity
And revise the particle position value

```
    }
     }
    End while
end while
    End for
```

5. Simulated Results

The obtained results, analysis, and simulation setup of the proposed EESRP are discussed in this section. For simulation testing, MATLAB 2018b software is used, and different parameters have been initialized, which includes accuracy, efficiency is calculated using this software. Trust optimization, key optimization and Firefly algorithm are evaluated individually, and their parameters are assessed and recorded. Similarly, the proposed hybrid algorithm is also evaluated, and the values are recorded. These values are compared existing method and results proven that the suggested model has higher efficiency. The initialized input parameters are discussed in **Table 2**.

Table 2. Simulation setup

Input parameter initialization	Values
Number of Nodes	100 nodes
Routing Protocol	AODV
Initial Energy of common node	100 J
Coverage Area	1500*1500
No of Attacker Nodes	10 nodes
Initial Energy of Cluster head node	1000 J
Cluster head nodes	10 nodes
Queue Type	Drop-Tail
Simulation Period	100 ms

5.1 The Simulation Results Evaluation Metric

The proposed EESRP routing protocol performance has been validated with the specific measurement of average energy consumption, end-to-end delay, PDR, routing overhead, and throughput of the routing protocol. Our primary focus is on the identification of the stable and reliable route along with the less energy, extended network lifetime and high signal strength. Also, the entire throughput is enhanced, which is higher than the traditional Ad Hoc On-Demand Distance Vector (AODV) protocol through delay data on the basis of energy and uniting the Signal Strength. The brief notes for evaluation of different metrics are discussed as follows:

5.1.1 Average Energy-Consumption

The Average Energy Consumption (AEC) of a network node has been measured by data transfer from source to a destination where an average quantity of energy is consumed to the ratio of transmitted data packets of the entire node. The measured results are represented unit as joules. The measure of energy consumption is mathematically written as,

$$AEC = \frac{Total\ energy\ consumed}{Total\ no.of\ available\ nodes} \quad (19)$$

5.1.2 Packet-Delivery Ratio (PDR)

The PDR is measured by the received packets ratio which is sent over the network. Also, the PDR value is utilized to measure the link stability of the network path. The network size is increased when the increase of network quantity. As a result, a high ratio of PDR represents an enhanced performance of routing protocol Baisakh [47] and offered better results. The mathematical representation of PDR is calculated by,

$$\text{PDR} = \frac{\sum \text{total number of received packets}}{\sum \text{totalnumber of transfered packets}} \quad (20)$$

5.1.3 Average Throughput

In this work, the throughput value is measured by the quantity of obtained bits at the receiver end. The mean throughput is calculated as throughput per unit duration. The network throughput also defined as the successive proportion of data packets delivered [48].

$$\text{T} = \frac{\text{Total number of receiving packets from node}}{\text{Data transmission period}} * 8 \quad (21)$$

5.1.4 Routing overhead Ratio

The routing overhead ratio is measured as the quantity of entire received data packets to the proportion of overall transmitted control packets. It is also known as Normalized Routing Overhead (NRO). Here the less overhead represents the better performance. It's mathematically written as,

$$\text{NRO} = \frac{\sum \text{total number of sent routing packets}}{\sum \text{ total number of received data packets}} \quad (22)$$

5.1.5 Average End-To-End Delay

The end-to-end delay is measured as the ratio of delay that occurs amongst data packets transfer from its source node to its endpoint. Here the delay comprises the route discovery time, propagating and transmitting time within WSNs, node's queuing delay and transmission delay at MAC layer [49]. The obtained results of the proposed system have been discussed in the following section.

5.2 Simulated Results

The proposed EESRP approach comprises of different stages, i.e. trust management, key management, and optimization method. During the simulation, the different nodes are randomly generated and pre-arranged in the form of a tree. The input parameters namely

distance and energy had been controlled and therefore, the length of the path was considered which led to the maintenance of lesser energy for a more extended period of time. This further increased the life of the network and helps in more efficient coverage. The node with the highest energy and the node that is farthest from the root is selected.

The node status is frequently updated due to the effective key management of routing protocol, the malicious nodes can be identified quickly. **Fig 2** clearly illustrates the performance of PSGR which is better than the HWMP. The suggested EESRP approach gives a better result than PSGR. In the proposed work, the design of trust management can isolate the malicious node and provided the assurance of trust route from source to the destination of a sensor network. Then data packets have been computed based on the trust value for a given set of associated pair values and neighbour nodes. This value exemplifies the degree of confidence where the neighbour node is consistent with regards to the delivered packet ratio.

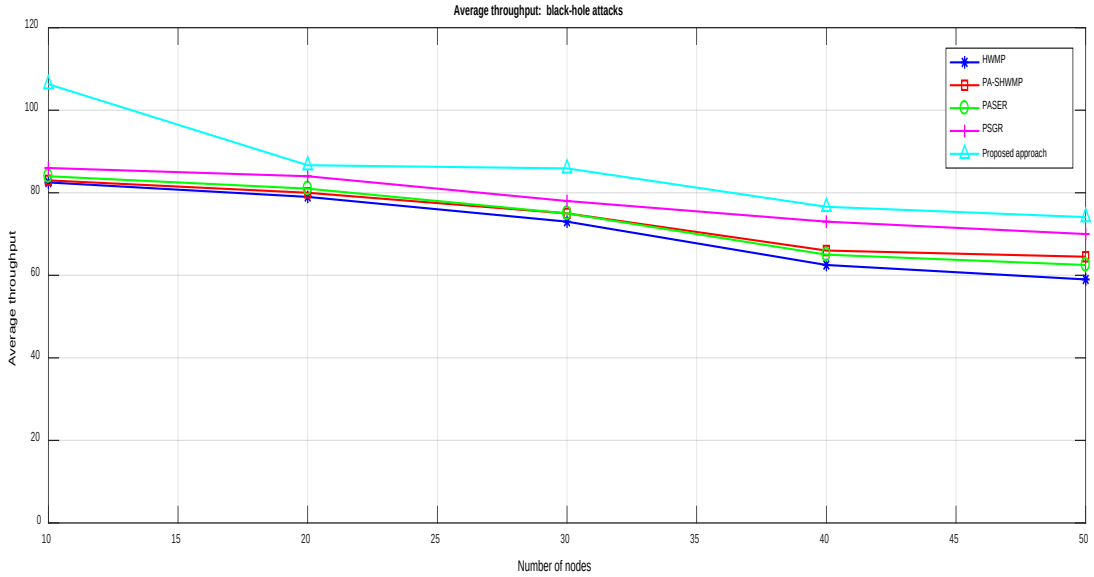

Fig. 2. Pictorial representation of Average throughput (EESRP with traditional technique)

Table 3 presents the PDR results, and if we increase the malicious nodes, the PDR ratio of the sensor node is minimized. In any case, the PDR under PSGR is superior to PA-SHWMP, HWMP and PASER. In addition, HWMP does not consider interior attacks and noxious hubs. With regard to this, we can't keep away from malignant hubs taking part in the steering; therefore, PDR is the most noticeably awful. When compared to PASER and PA-SHWMP, the malicious hubs are avoided from the system which is not long after they have been identified, which results in fewer hubs can take an interest in the steering and PDR of PA-SHWMP and PASER diminishes quickly when the quantity of malignant hubs increments. Nonetheless, in the proposed EESRP routing protocol, the dynamic notoriety system recognizes the harmful hubs, which is more precise when compared to the PASER and PA-SHWMP.

Table 3. Simulated Results of Average Throughput and Average PDR

Author \ Number of Nodes	Average throughput: black-hole attacks						Average PDR					
	0	10	20	30	40	50	0	10	20	30	40	50
HWMP Khabbazian et al [50]	83.5	82.5	79	73	62.5	59	88	71	66	52.5	32	27
PA-SHWMP Lin et al. [51]	85	83	80	75	66	64.5	90	76	70	58	42.5	32
PASER Sbeiti et al. [52]	87	84	81	75	65	62.5	91	80	75	62	50	40
PSGR Lin et al. [53]	88.5	86	84	78	73	70	92	88	80	70	62	61
EESRP	91.3	86.7	85.9	79.6	74.1	72	93.6	89.3	82.4	73	63.5	62.5

The simulated results were absorbed by utilizing 5 to 10 source-sink sets to think about the normal ED of the four conventions. **Fig. 3** clearly illustrates that the traffic loads under less or medium condition, the network delay is lower than 200 ms, but in the case of high or heavy traffic loads, the network consists of more nodes and relay achieve almost 250ms. In addition to this, the average ratio of end delay is a little bit high in PSGR when compared to the traditional method, namely PASER, HWMP and PA-SHWMP. Further, this work has detected and isolated the malevolent node that resulted in higher network delay, which requires the routing security protocol. For this, the cryptography technique is incorporated and through this, the unique ID has been generated; thereby minimizing the routing overhead and network delay ratio.

In addition, the EESRP performs the combination of trust; key and optimization toward offer less energy-consuming devices and maintain the privacy preservation network packets. At the end of the simulation, the average ratio of “end to end delay” in EESRP is higher than the performance of those of PSGR, PA-SHWMP, HWMP and PASER (shown in **Fig. 4**). Also, the trade-off between the network is better throughput, energy efficiency and packet delivery ratio. In our protocol, select the cluster head on the basis of fuzzy rule and clusters that uses the node centrality as input parameters. Here each node in the in-network chooses the channel with the least cost and joins it. This will support extending the network lifetime than the traditional method. On the other hand, the lifetime of the network nodes is increased and reduced the consumed power in the proposed network. By the suggested technique, the average energy consumption has been measured and discussed in **Table 4**.

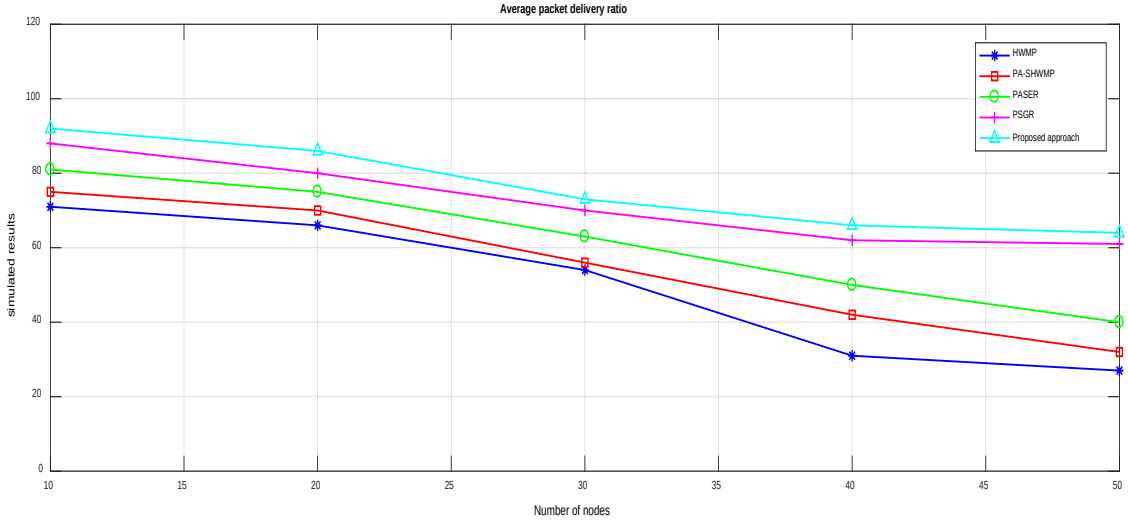

Fig. 3. Pictorial representation of Average packet delivery ratio (EESRP approach with traditional technique)

Table 4. Simulated Results of End-to-End delay and Average Energy-Consumption

Number of hubs / Researcher	Average End-to-End Delay					Average energy consumption				
	2	4	6	8	10	2	4	6	8	10
HWMP Khabbazian et al [50]	40	80	119	138	180	1.2	1.8	2.8	3.8	5
PA-SHWMP Lin et al. [51] **PASER Sbeiti et al.** [52]	48	100	130	148	222	1.7	2.4	3.6	5	6.8
PSGR Lin et al. [53]	42	90	122	140	200	1.4	2	3.4	4.2	5.9
HWMP Khabbazian et al [50] **PA-SHWMP Lin et al.** [51]	60	118	136	162	237	0.9	1.2	2	2.8	5.1
PASER Sbeiti et al. [52]	78	139	152	193	261	0.79	1	1.5	2.67	3.5

In addition, the EESRP performs the combination of trust; key and optimization toward offer less energy-consuming devices and maintain the privacy preservation network packets. At the end of the simulation, the average ratio of “end to end delay” in EESRP was higher than the performance of PSGR, PA-SHWMP, HWMP and PASER. Also, the trade-off between the network is better throughput, energy efficiency and, packet delivery ratio. In our protocol, select the cluster head on the basis of fuzzy rule and clusters that uses the node centrality as input parameters. Here each node in the in-network chooses the channel with the least cost and joins it. This will support extending the network lifetime than the traditional method. On the other hand, the lifetime of the network nodes is increased and reduced the consumed power in the proposed network. By the suggested technique, the average energy consumption has been measured and discussed in **Table 4**.

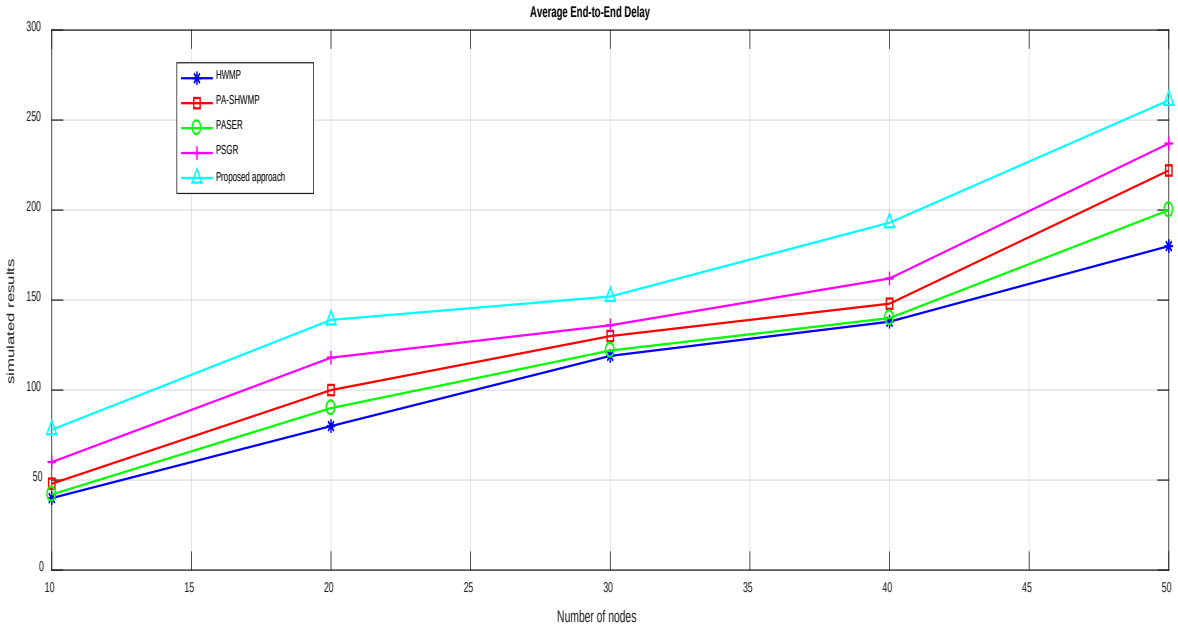

Fig. 4. Pictorial Representation of End to End Delay (EESRP With Traditional Technique)

The results illustrate the attained results from the simulation experimentations with 2-15 sets of source-destination network nodes toward relating the ratio of energy consumption and the presented approaches, namely EESRP, PA-SHWMP, HWMP and PASER, PSGR. **Fig. 5** illustrates that the suggested method in the sensor network dramatically affected the performance of energy consumption via network hubs.

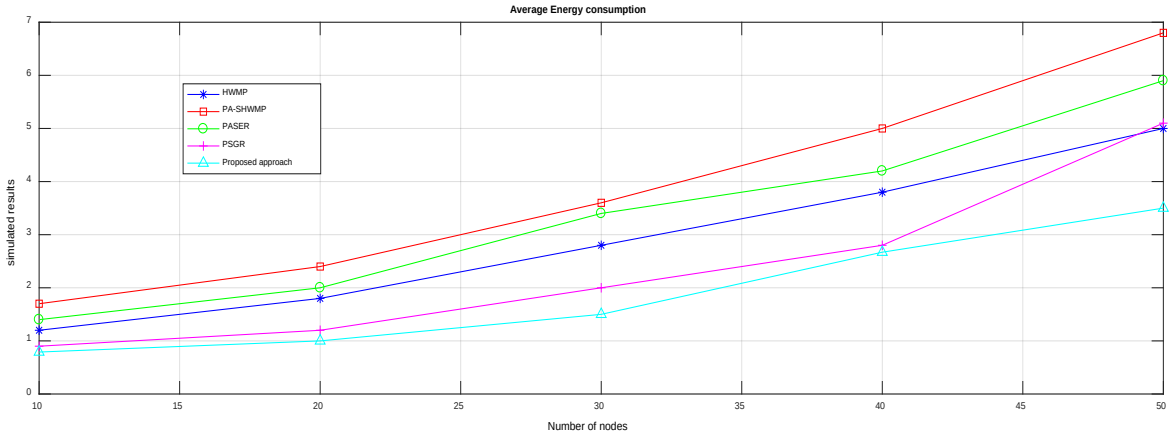

Fig. 5. Pictorial Representation of Average Energy Consumption (EESRP Approach with Traditional Technique)

The average energy consumption is increased for all the routing protocols as the number of hop increases. But, in the routing process, the performance of energy consumption has been taken into consideration which shows the proposed EESRP gives better results when compared to the traditional approach namely PSGR, PASER, HWMP and PA-SHWMP.

Table 5. Energy consumed of WSN in static mode of operation

Energy consumed (mJ)	AODV Govindasamy and Punniakody [54]	EESRP
Transmit Mode	1.080135	1.0632
Receive mode	9.394479	8.691
Idle mode	17.9158	15.673

Table 5 presents the obtained results of WSN in static mode operation, which includes energy consumption of transmitting node, receive node and idle modes. From the listed values in the table, we observed that the proposed protocol has less energy consumption than AODV. Therefore, we concluded that the proposed EESRP protocol has better performance than that of AODV specific to the energy consumption of a network.

6. Discussion

Communication overhead is the amount of time spent communicating with the nodes. It is the combination of different resources like the memory, bandwidth and computational time that are necessary for performing a task. In cluster formation, if the channel between the nodes is secure, a random number is encrypted then sent between the nodes and an acknowledgement is received from the other node. This acknowledgement is referred to as ACK, and its size is 1 bit. The secure channel is bidirectional; hence data flow has been mainlined in both directions. From the results, it can be seen that the communication overhead for the suggested method decreased since more communication takes place at a time.

In the suggested EESRP routing protocol, the average throughput ratio is measured based on the data packets that have been transmitted from sender to receiver node at a specified amount of time. An increase in data packets leads to an increase in each node per time resulting in increased throughput in the routing network. However, this depends on the trust score and key generation of each node. Through simulation, the obtained results are discussed and compared with the performance with the traditional method.

The average throughputs and PDR of routing protocol is given in the previous section, where the throughput is affected through the occurrence of malevolent nodes in the black-hole attack. The performance of an EESRP system is validated and related with the traditional method such as PSGR (secure aware, privacy-aware and green routing procedure), PA-SHWMP (Privacy- Secure aware Hybrid Wireless Mesh Protocol), PASER and HWMP (hybrid wireless mesh networks). Thus, the traditional technique established the route based on reputation approach along with cryptography technique that might be avoided and identify the malicious nodes which are participated in the routing protocol. Whereas, the PASER technique relies on the origin, dynamic key management and neighbour authentication scheme. In addition to this, most of the trusted nodes are dynamically occupying the routing module as well as effectively forwarded the data when the malicious nodes are lesser than 30 % using the PASER technique compared to the PA-SHWMP scheme. To isolate and identify the malevolent nodes, the EESRP method uses the effective key management scheme which frequently updates the node status rapidly and effectively. Furthermore, more internal nodes are captured when a fraction of malicious sensor nodes is greater than 30 % of the system.

The results in malicious hubs with less importance of data security are prohibited from the system, and the remaining hub will be compelled to collaborate. With regard to this, the more precise distinguishing proof of malicious hubs and higher the ratio of malicious hubs lead to the preferable PDR execution of EESRP over that of PSGR, PASER and PA-SHWMP. The proposed EESRP routing schemes deliver a message to another node between a group of nodes especially, one sensor node is nearest to the source as well forward the packet to that node immediately, which is a unique way to reduce the end-to-end delay. Generally, the end-to-end delay is due to this received sink once the event occurs, whereas the delay will happen. Based on the unique trust value, the node generates one packet at a time as well as captured the reports of delay of event data in the network. If the network path can stay awake for a while first packets are sent in the same manner. At each node, the subsequent data packets do not require to support the wake-up delay, so the end of the packet to end delay is less than the first data packet.

To improve the power consumption at each node, our proposed routing protocol takes care of transmits to the nodes and distance among the nodes with the least distance at the time of route selection. Hence the energy consumption can be reduced between the nodes. Moreover, the location/position of each node has been calculated that confines the extent used for finding novel routes to a reduced region, hence reducing energy consumption. This location information can minimize the search area for the route, so there is a huge decrease in energy consumption along with several routing messages. The pictorial representation of energy consumption vs mode of action is shown in **Fig. 6**.

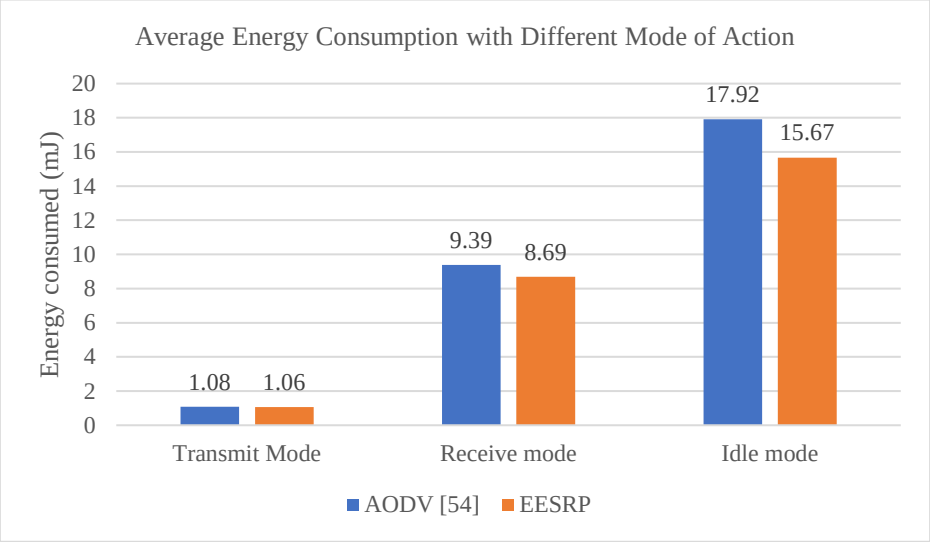

Fig. 6. Performance Related to Average Energy Consumption with Different Mode of Action

Then we calculated the trust score of each node on the basis of its location, updated trust value, node honesty, frequently visited nodes and energy of nodes whereas the trust score is utilized to obtain the optimal route of the network between the source and destination node. Subsequently, selected a higher trust score of sensor node and formed the cluster based on the cluster head. In addition, node behaviour has been monitored by trust value or trust management. All the nodes monitor one or more behavioural aspects of their neighbour nodes toward detecting misbehaviour nodes. These behavioural aspects are used to detect a trust

metric when the trust metric is inter-link with the trust value. The total trust score is measured by combining direct and indirect trust scores, whereas the indirect value measured by opinion on other nodes trustworthiness and direct trust value is calculated by nodes self-observations. The performance of the trust management is measured by packet drop rate, the packet transmitted rate and receiver rate. On the other hand, describe whether it's a successful transmission or a failure. Based on the suggested optimization method (hybrid PSO and HS) to balances energy load between different network nodes path selection hence the energy of each sensor node has been reduced, thus increasing the network life.

7. Conclusion and Future Work

This study presents an energy-efficient based secure routing protocol by combining trust management, key management, and optimization technique. Furthermore, cluster formation, and feature selection technique has been performed for obtaining an optimal solution. The suggested techniques have also been simulated using MATLAB 2018b simulation software, and different performance metrics are evaluated, and compared with the traditional method. Specifically, the trust value of the neighbour node was calculated, which increases the search space and minimize the distance. The simulation results have proven that, the average ratio of "end to end delay" in EESRP is higher than the performance of PSGR, PA-SHWMP, HWMP and PASER. Also, the trade-off between the network is better throughput, energy efficiency and packet delivery ratio. But, the routing process, the performance of energy consumption has been taken into consideration which shows the proposed EESRP provides better results when related to the traditional method. From the obtained results, the suggested EESRP protocol performance has been estimated as well as it is proven that the proposed EESRP approach has higher efficiency, accuracy and energy is meagre. The suggested framework is applicable to intrusion detection and trust-based routing application which monitors the real-time data. In future, the presented model will be extended to various types of WSNs such as heterogeneous and dynamic WSNs and will validate the performance of sensor nodes and data transmission. Also, the security of the algorithm can be further explored and analysed to identify the security level of the algorithm.

Conflict of Interest

The author declares that they have no known competing financial interest or personal relationship that could have appeared to influence the work reported in this paper.

Funding acknowledgment

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] M. Hawa, K. A. Darabkh, R. Al-Zubi, and G. Al-Sukkar, “A Self-Learning MAC Protocol for Energy Harvesting and Spectrum Access in Cognitive Radio Sensor Networks,” *J. Sensors*, vol. 2016, pp. 1–18, 2016. Article (CrossRef Link).

[2] K. A. Darabkh, W. Y. Albtoush, and I. F. Jafar, “Improved clustering algorithms for target tracking in wireless sensor networks,” *J. Supercomput.*, vol. 73, no. 5, pp. 1952–1977, May 2017. Article (CrossRef Link).

[3] G. P. Gupta, M. Misra, and K. Garg, “Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks,” *J. Netw. Comput. Appl.*, vol. 41, pp. 300–311, May 2014. Article (CrossRef Link).

[4] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in *Proc. of the 33rd Annual Hawaii International Conference on System Sciences*, vol. vol.1, p. 10, 2000. Article (CrossRef Link).

[5] V. Sivaprasatham and J. Venkateswaran, “A Secure Key Management Technique for Wireless Body Area Networks,” *J. Comput. Sci.*, vol. 8, no. 11, pp. 1780–1787, Nov. 2012. Article (CrossRef Link).

[6] M. Masdari and S. Ahmadzadeh, “Comprehensive analysis of the authentication methods in wireless body area networks,” *Secur. Commun. Networks*, vol. 9, no. 17, pp. 4777–4803, Nov. 2016. Article (CrossRef Link).

[7] S. Sankaran, M. Husain, and R. Sridhar, “IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Networks,” in *Proc. of 5th Annu. Symp. Inf. Assur.*, 2009.

[8] D. M. Barakah and M. Ammad-uddin, “A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of a Virtual Doctor Server in Existing Architecture,” in *Proc. of 2012 Third International Conference on Intelligent Systems Modelling and Simulation*, pp. 214–219, Feb. 2012. Article (CrossRef Link).

[9] N. Bradai, L. Chaari, and L. Kamoun, “A Comprehensive Overview of Wireless Body Area Networks (WBAN),” *Int. J. E-Health Med. Commun.*, vol. 2, no. 3, pp. 1–30, Jul. 2011. Article (CrossRef Link).

[10] S. N. Ramli and R. Ahmad, “Surveying the Wireless Body Area Network in the realm of wireless communication,” in *Proc. of 2011 7th International Conference on Information Assurance and Security (IAS)*, pp. 58–61, Dec. 2011. Article (CrossRef Link).

[11] S. Saleem, S. Ullah, and H. Seon Yoo, "On the Security Issues in Wireless Body Area Networks," vol. 3, 2009.

[12] K. K. Khaing and K. M. M. Aung, “Secured Key Distribution Scheme for Cryptographic Key Management System,” in *Proc. of 2010 International Conference on Availability, Reliability and Security*, pp. 481–486, Feb. 2010. Article (CrossRef Link).

[13] D. Satish kumar, N. Nagarajan, and A. Taher Azar, “An Improved Key Management Scheme with High Security in Wireless Sensor Networks,” *Mobile Ad-Hoc and Sensor Networks. MSN 2007. Lecture Notes in Computer Science*, pp. 249–264, 2014. Article (CrossRef Link).

[14] N. Bradai, S. Belhaj, L. Chaari, and L. Kamoun, “Study of medium access mechanisms under IEEE 802.15.6 standard,” in *Proc. of 2011 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2011)*, pp. 1–6, Oct. 2011. Article (CrossRef Link).

[15] Z. Jin, Y. Jian-Ping, Z. Si-Wang, L. Ya-Ping, and L. Guang, “A Survey on Position-Based Routing Algorithms in Wireless Sensor Networks,” *Algorithms*, vol. 2, no. 1, pp. 158–182, Feb. 2009. Article (CrossRef Link).

[16] S. Nikoletseas and P. Spirakis, “Probabilistic Distributed Algorithms for Energy Efficient Routing and Tracking in Wireless Sensor Networks,” *Algorithms*, vol. 2, no. 1, pp. 121–157, Feb. 2009. Article (CrossRef Link).

[17] A. Alemdar and M. Ibnkahla, “Wireless sensor networks: Applications and challenges,” in *Proc. of 2007 9th International Symposium on Signal Processing and Its Applications*, pp. 1–6, Feb. 2007. Article (CrossRef Link).

[18] T. Amgoth and P. K. Jana, "Energy-aware routing algorithm for wireless sensor networks," *Comput. Electr. Eng.*, vol. 41, pp. 357–367, Jan. 2015. Article (CrossRef Link).
[19] W. Zhang, G. Han, Y. Feng, and J. Lloret, "IRPL: An energy efficient routing protocol for wireless sensor networks," *J. Syst. Archit.*, vol. 75, pp. 35–49, Apr. 2017. Article (CrossRef Link).
[20] S. B. Lande and S. Z. Kawale, "Energy Efficient Routing Protocol for Wireless Sensor Networks," in *Proc. of 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 77–81, Dec. 2016. Article (CrossRef Link).
[21] H.-H. Liu, J.-J. Su, and C.-F. Chou, "On Energy-Efficient Straight-Line Routing Protocol for Wireless Sensor Networks," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2374–2382, Dec. 2017. Article (CrossRef Link).
[22] K. Muthukumaran, K. Chitra, and C.Selvakumar, "An energy efficient clustering scheme using multilevel routing for wireless sensor network," *Comput. Electr. Eng.*, vol. 69, pp. 642-652, Jul. 2018. Article (CrossRef Link).
[23] K. A. Darabkh, N. J. Al-Maaitah, I. F. Jafar, and A. F. Khalifeh, "EA-CRP: A Novel Energy-aware Clustering and Routing Protocol in Wireless Sensor Networks," *Comput. Electr. Eng.*, vol. 72, pp. 702-718, Nov. 2018. Article (CrossRef Link).
[24] S. Nikolidakis, D. Kandris, D. Vergados, and C. Douligeris, "Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering," *Algorithms*, vol. 6, no. 1, pp. 29–42, Jan. 2013. Article (CrossRef Link).
[25] R. Sujee and K. E. Kannammal, "Energy efficient adaptive clustering protocol based on genetic algorithm and genetic algorithm inter cluster communication for wireless sensor networks," in *Proc. of 2017 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–6, Jan. 2017, Article (CrossRef Link).
[26] P. Khatri, "Using identity and trust with key management for achieving security in Ad hoc Networks," in *Proc. of 2014 IEEE International Advance Computing Conference (IACC)*, pp. 271–275, Feb. 2014. Article (CrossRef Link).
[27] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," *IEEE Trans. Netw. Serv. Manag.*, vol. 9, no. 2, pp. 169–183, Jun. 2012. Article (CrossRef Link).
[28] S. Dhanalakshmi and M. Sathiya, "An Improved Ant Based Routing Technique in WSN with High Security," no. September, pp. 1771–1778, 2015.
[29] D. Srinath, V. Subedha, and S. Venkatraman, "ACO based mobile agent for secured key management in manet," *ARPN J. Eng. Appl. Sci.*, vol. 10, no. 11, pp. 4877–4881, 2015.
[30] S. Ganesh, "Efficient and Secure Routing Protocol for WSN-A Thesis," 2017.
[31] T. Rahayu, S.-G. Lee, and H.-J. Lee, "A Secure Routing Protocol for Wireless Sensor Networks Considering Secure Data Aggregation," *Sensors*, vol. 15, no. 7, pp. 15127–15158, Jun. 2015. Article (CrossRef Link).
[32] N. Sharma, B. M. Singh, and K. Singh, "QoS-based energy-efficient protocols for wireless sensor network," *Sustain. Comput. Informatics Syst.*, vol. 30, p. 100425, Jun. 2021. Article (CrossRef Link).
[33] D. Mehta and S. Saxena, "MCH-EOR: Multi-objective Cluster Head Based Energy-aware Optimized Routing algorithm in Wireless Sensor Networks," *Sustain. Comput. Informatics Syst.*, vol. 28, p. 100406, Dec. 2020. Article (CrossRef Link).
[34] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks," *Appl. Soft Comput.*, vol. 77, pp. 366–375, Apr. 2019. Article (CrossRef Link).
[35] P. C. S. Rao, P. K. Jana, and H. Banka, "A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks," *Wirel. Networks*, vol. 23, no. 7, pp. 2005–2020, Oct. 2017. Article (CrossRef Link).
[36] M. A. Adnan, M. A. Razzaque, M. A. Abedin, S. M. Salim Reza, and M. R. Hussein, "A Novel Cuckoo Search Based Clustering Algorithm for Wireless Sensor Networks," pp. 621–634, 2016.

[37] R. S. Y. Elhabyan and M. C. E. Yagoub, "Two-tier particle swarm optimization protocol for clustering and routing in wireless sensor network," *J. Netw. Comput. Appl.*, vol. 52, pp. 116–128, Jun. 2015. Article (CrossRef Link).

[38] G. P. Gupta and S. Jha, "Integrated clustering and routing protocol for wireless sensor networks using Cuckoo and Harmony Search based metaheuristic techniques," *Eng. Appl. Artif. Intell.*, vol. 68, pp. 101–109, Feb. 2018. Article (CrossRef Link).

[39] M. Ahmadi, M. Shojafar, A. Khademzadeh, K. Badie, and R. Tavoli, "A Hybrid Algorithm for Preserving Energy and Delay Routing in Mobile Ad-Hoc Networks," *Wirel. Pers. Commun.*, vol. 85, no. 4, pp. 2485–2505, Dec. 2015. Article (CrossRef Link).

[40] L. Sheng, J. Shao, and J. Ding, "A Novel Energy-Efficient Approach to DSR Based Routing Protocol for Ad Hoc Network," in *Proc. of 2010 International Conference on Electrical and Control Engineering*, pp. 2618–2620, Jun. 2010. Article (CrossRef Link).

[41] Sugandh and R. Panday, "Energy Efficient-Long Life LEACH Variant Protocol for MANET Environment," *Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. 5, pp. 2320–2325, 2016.

[42] F. T. Zuhra, K. A. Bakar, A. Ahmed, and M. A. Tunio, "Routing protocols in wireless body sensor networks: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 99, pp. 73–97, Dec. 2017. Article (CrossRef Link).

[43] S. Sridhar, R. Baskaran, R. Anitha, R. Sankar, "Proficient and secured routing in MANET based on trust and energy supported AODV," *Appl. Math. Inf. Sci.*, vol. 11, no. 3, pp. 807–817, 2017. Article (CrossRef Link).

[44] M. Sheikhan and E. Hemmati, "PSO-Optimized Hopfield Neural Network-Based Multipath Routing for Mobile Ad-hoc Networks," *Int. J. Comput. Intell. Syst.*, vol. 5, no. 3, pp. 568–581, 2012.

[45] Y. Shi and R. Eberhart, "Parameter selection in particle swarm optimization," in *Proc. of Proc. 7th Int. Conf. Evolutionary Programming*, pp. 591–601, 1998.

[46] R. PushpaLakshmi, P. Lavanya, and S. Bhuvaneshwari, "Survey of ACO and PSO based Secure Routing protocols for Wireless networks," *Int. J. Adv. Res. Sci. Eng.*, vol. 6, no. 12, pp. 820–832, 2017.

[47] B. Baisakh, "A Review of Energy Efficient Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," *Int. J. Comput. Appl.*, vol. 68, no. 20, pp. 6–15, Apr. 2013. Article (CrossRef Link).

[48] A. Behera and A. Panigrahi, "Determining the Network Throughput and Flow Rate Using GSR and AAL2R," *Int. J. UbiComp*, vol. 6, no. 3, pp. 9–18, Jul. 2015. Article (CrossRef Link).

[49] S. Sharma and P. S. Patheja, "Improving AODV Routing Protocol with Priority and Power Efficiency in Mobile Ad hoc WiMAX Network," *Int. J. Comput. Technol. Electron. Eng.*, vol. 2, no. 1, pp. 87–93, 2002.

[50] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," *IEEE Trans. Wirel. Commun.*, vol. 8, no. 2, pp. 736–745, Feb. 2009. Article (CrossRef Link).

[51] H. Lin, J. Ma, J. Hu, and K. Yang, "PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 2012, no. 1, p. 69, Dec. 2012. Article (CrossRef Link).

[52] M. Sbeiti, N. Goddemeier, D. Behnke, and C. Wietfeld, "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 3, pp. 1950–1964, Mar. 2016. Article (CrossRef Link).

[53] H. Lin, J. Hu, L. Xu, Y. Tian, L. Liu, and S. Blakeway, "A trustworthy and energy-aware routing protocol in software-defined wireless mesh networks," *Comput. Electr. Eng.*, vol. 64, pp. 407–419, Nov. 2017. Article (CrossRef Link).

[54] J. Govindasamy and S. Punniakody, "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack," *J. Electr. Syst. Inf. Technol.*, vol. 5, no. 3, pp. 735–744, Dec. 2018. Article (CrossRef Link).

Ms.S.Sudha Mercy is currently working as Assistant Professor in Jeppiaar Institute of Technology, Chennai, India. She completed her B.Tech(IT) at Anna University in 2011 and Post Graduation M.E(CSE) at Anna University in 2013.She is currently pursuing Ph.D at Anna University. She has 5.2 years of Teaching Experience. She has handled various subjects like Design and Analysis of Algorithm, Data Structures, C Programming, Object Oriented programming, Total Quality Management, Problem Solving and Python Programming, Internet Programming, Computer Networks. Her research interest include Wireless Sensor Networks, Network Security and Datascience. She is well skilled in programming languages. She completed 6 online courses, industry-oriented internships, attended many workshops and Faculty Development program. She published books in Total Quality Management, Object Oriented Programming, Compiler Design and Problem Solving and Python Programming. She has published papers in International Journals and has presented papers in International Conferences.

Dr.J.M.Mathana obtained her B.E Degree in Electronics and Communication Engineering, M.E Degree in VLSI Design and Ph.D Degree in Information and Communication from Anna University, Chennai, India. She has over 31 years of rich experience in academic arena and industry. She has developed a wide range of skills that would meet and exceed the expectations for her current role on the leverage of her blend of experience in academic as well as industry. Currently, she is working as Professor & Dean Engg and Technology in St.Peter's Institute of Higher Education and Research Chennai, India. Her research interests include the Error Corrective Coding, Interleavers, Networks, Medical Electronics and VLSI Design. Her strong commitment towards research is reflected in her contribution of more than 118 international and national publications. She is the distinguished member of the Indian Society of Technical Education and Senior member of IEEE. She is a visionary leader and good administrator to manage educational transformation in the institution to develop high academic appreciation in a background of super postural care and to make a real difference to student's lives in a totally innovative education setting. Her objective is to pursue a challenging career and be a part of a progressive organization that gives scope to enhance her knowledge, research, skills and hard work.

Dr. J.S Leena Jasmine, obtained Doctorate degree from Jawaharlal Nehru Technological University, Hyderabad in the area of Digital Image Processing in 2015, M.E. degree in "Applied Electronics" from Hindustan College of Engineering affiliated to University of Madras in 1999 and B.E Degree in "Electronics & Communication Engineering" from Indian Engineering College affiliated to Madurai Kamaraj University in 1993. She has 23 years of teaching in reputed Institutes. She has participated, and presented papers at various conferences in India. She has published papers in peer reviewed national and international journals. She has published books on various subjects like Digital Image Processing, Microprocessor and Microcontroller, Linear Integrated Circuits, Electronic Circuits and Computer Architecture. She also holds recognition for Research Supervisor under Anna University for P.hd Guidance. Her research interests are Digital Image Processing, Embedded System and Data Mining.